

Unique Parallel Decomposition in Branching and Weak Bisimulation Semantics

Bas Luttik

Abstract

We consider the property of unique parallel decomposition modulo branching and weak bisimilarity. First, we show that infinite behaviours may fail to have parallel decompositions at all. Then, we prove that totally normed behaviours always have parallel decompositions, but that these are not necessarily unique. Finally, we establish that weakly bounded behaviours have unique parallel decompositions. We derive the latter result from a general theorem about unique decompositions in partial commutative monoids.

1 Introduction

A recurring question in process theory is to what extent the behaviours definable in a certain process calculus admit a unique decomposition into indecomposable parallel components. Milner and Moller [15] were the first to address the question. They proved a unique parallel decomposition theorem for a simple process calculus, which allows the specification of finite behaviour up to strong bisimilarity and includes parallel composition in the form of pure interleaving without interaction between the components. They also presented counterexamples showing that unique parallel decomposition may fail in process calculi in which it is possible to specify infinite behaviour, or in which certain coarser notions of behavioural equivalence are used.

Moller proved several more unique parallel decomposition results in his dissertation [16], replacing interleaving parallel composition by CCS parallel composition, and then also considering weak bisimilarity. These results were established with subsequent adaptations of an ingenious proof technique attributed to Milner. Christensen, in his dissertation [3], further adapted the proof technique to make it work for the weakly normed behaviours recursively definable modulo strong bisimilarity, and for all behaviours recursively definable modulo distributed bisimilarity.

With each successive adaptation of Milner's proof technique, the technical details became more complicated, but the general idea of the proof remained the same. In [12] we, therefore, made an attempt to isolate the deep insights from the technical details, by identifying a sufficient condition on partial commutative monoids that facilitates an abstract version of Milner's proof technique. To concisely present the sufficient condition, we put forward the notion of *decomposition order*; it is established in [12] by means of an abstract version of Milner's technique, that if a partial commutative monoid can be endowed with a decomposition order, then it has unique decomposition.

Application of the general result of [12] in commutative monoids of behaviour is often straightforward: a well-founded order naturally induced on behaviour by (a terminating fragment of) the transition relation typically satisfies the properties of a decomposition order. All the aforementioned unique parallel decomposition results can be directly obtained in this way, except Moller's result that finite behaviours modulo weak bisimilarity have unique decomposition. It turns out that a decomposition order cannot straightforwardly be obtained from the transition relation if

certain transitions are deemed unobservable by the behavioural equivalence under consideration.

In this paper, we address the question of how to establish unique parallel decomposition in settings with a notion of unobservable behaviour. Our main contribution will be an adaptation of the general result in [12] to make it suitable for establishing unique parallel decomposition results also in settings with a notion of unobservable behaviour. To illustrate the result, we shall apply it to establish unique parallel decomposition for finite behaviour modulo branching or weak bisimilarity. We shall also show, by means of a counterexample, that unique parallel decomposition fails for infinite behaviours modulo branching and weak bisimilarity, even if only a very limited form of infinite behaviour is considered (totally normed behaviour definable in a process calculus with prefix iteration).

A positive answer to the unique parallel decomposition question seems to be mainly of theoretical interest. It yields a convenient tool for proving other theoretical properties of interest about process calculi. For instance, Møller's proofs in [17, 18] that PA and CCS cannot be finitely axiomatised without auxiliary operations, Hirshfeld and Jerrum's proof in [10] that bisimilarity is decidable for normed PA, and the completeness proofs for the equational axiomatisations of PA and CCS with auxiliary operations in [6] and [1], all rely on the property of unique parallel decomposition. Nevertheless, an answer to the question could be of practical interest too, e.g., to devise methods for finding the maximally parallel implementation of a behaviour [4], or to improve verification methods [9].

This paper is organised as follows. In Section 2 we introduce the simple process calculus that we shall use to illustrate our theory of unique decomposition. There, we also present counterexamples to the effect that infinite behaviours in general may not have a decomposition, and totally normed behaviours may have more than one decomposition. In Section 3 we recap the theory of decomposition put forward in [12] and discuss why it is not readily applicable to establish unique parallel decomposition for finite behaviours modulo branching and weak bisimilarity. In Section 4 we adapt the theory of [12] to make it suitable for proving unique parallel decomposition results in process calculi with a notion of unobservability. We end the paper in Section 5 with a short conclusion.

2 Processes up to branching and weak bisimilarity

We define a simple language of process expressions together with an operational semantics, and notions of branching and weak bisimilarity. We shall then investigate to what extent process expressions modulo branching or weak bisimilarity admit parallel decompositions. We shall present examples of process expressions without a decomposition, and of totally normed process expressions with two distinct decompositions.

Syntax We fix a set \mathcal{A} of *actions*, and declare a special action τ that we assume is not in \mathcal{A} . We denote by \mathcal{A}_τ the set $\mathcal{A} \cup \{\tau\}$, and we let a range over \mathcal{A} and α over \mathcal{A}_τ . The set \mathcal{P} of *process expressions* is generated by the following grammar:

$$P ::= \mathbf{0} \mid \alpha.P \mid P + P \mid P \parallel P \mid \alpha^*P \quad (\alpha \in \mathcal{A}_\tau).$$

The language above is BCCS (the core of Milner's CCS [13]) extended with a construction $_ \parallel _$ to express interleaving parallelism and the prefix iteration construction $\alpha^* _$ to be able to specify a restricted form of infinite behaviour. To be able to omit some parentheses when writing process expressions, we adopt the convention that $\alpha.$ and α^* bind stronger, and $+$ binds weaker than all the other operations.

$$\begin{array}{cccc}
\frac{}{\alpha.P \xrightarrow{\alpha} P} & \frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'} & \frac{Q \xrightarrow{\alpha} Q'}{P+Q \xrightarrow{\alpha} Q'} & \\
\frac{P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q} & \frac{Q \xrightarrow{\alpha} Q'}{P \parallel Q \xrightarrow{\alpha} P \parallel Q'} & \frac{}{\alpha^*P \xrightarrow{\alpha} \alpha^*P} & \frac{P \xrightarrow{\alpha} P'}{\alpha^*P \xrightarrow{\alpha} \alpha^*P'}
\end{array}$$

Table 1: The operational semantics.

Operational semantics and branching and weak bisimilarity We define on \mathcal{P} binary relations $\xrightarrow{\alpha}$ ($\alpha \in \mathcal{A}_\tau$) by means of the transition system specification in Table 1. We shall henceforth write $P \longrightarrow P'$ if there exist P_0, \dots, P_n ($n \geq 0$) such that $P = P_0 \xrightarrow{\tau} \dots \xrightarrow{\tau} P_n = P'$. Furthermore, we shall write $P \xrightarrow{(\alpha)} P'$ if $P \xrightarrow{\alpha} P'$ or $\alpha = \tau$ and $P = P'$.

Definition 1 (Branching bisimilarity [8]). A symmetric binary relation \mathcal{R} on \mathcal{P} is a *branching bisimulation* if for all $P, Q \in \mathcal{P}$ such that $P \mathcal{R} Q$ and for all $\alpha \in \mathcal{A}_\tau$ it holds that

$$\text{if } P \xrightarrow{\alpha} P' \text{ for some } P' \in \mathcal{P}, \text{ then there exist } Q'', Q' \in \mathcal{P} \text{ such that } Q \longrightarrow Q'' \xrightarrow{(\alpha)} Q' \text{ and } P \mathcal{R} Q'' \text{ and } P' \mathcal{R} Q'.$$

We write $P \dot{\equiv}_b Q$ if there exists a branching bisimulation \mathcal{R} such that $P \mathcal{R} Q$.

The relation $\dot{\equiv}_b$ is an equivalence relation on \mathcal{P} (this is not as trivial as one might expect; for a proof see [2]). It is also compatible with the construction of parallel composition in our syntax, which means that, for all $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$:

$$P_1 \dot{\equiv}_b Q_1 \text{ and } P_2 \dot{\equiv}_b Q_2 \text{ implies } P_1 \parallel P_2 \dot{\equiv}_b Q_1 \parallel Q_2. \quad (1)$$

(The relation $\dot{\equiv}_b$ is also compatible with α ., but not with $+$ and α^* . In this paper, we shall only rely on compatibility with \parallel .)

Definition 2 (Weak bisimilarity [14]). A symmetric binary relation \mathcal{R} on \mathcal{P} is a *weak bisimulation* if for all $P, Q \in \mathcal{P}$ such that $P \mathcal{R} Q$ and for all $\alpha \in \mathcal{A}_\tau$ it holds that

$$\text{if } P \xrightarrow{\alpha} P' \text{ for some } P' \in \mathcal{P}, \text{ then there exist } Q', Q'', Q''' \in \mathcal{P} \text{ such that } Q \longrightarrow Q'' \xrightarrow{(\alpha)} Q''' \longrightarrow Q' \text{ and } P' \mathcal{R} Q'.$$

We write $P \dot{\equiv}_w Q$ if there exists a weak bisimulation \mathcal{R} such that $P \mathcal{R} Q$.

The relation $\dot{\equiv}_w$ is an equivalence relation on \mathcal{P} . It is also compatible with parallel composition, i.e., for all $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$:

$$P_1 \dot{\equiv}_w Q_1 \text{ and } P_2 \dot{\equiv}_w Q_2 \text{ implies } P_1 \parallel P_2 \dot{\equiv}_w Q_1 \parallel Q_2. \quad (2)$$

(Just like $\dot{\equiv}_b$, the relation $\dot{\equiv}_w$ is also not compatible with $+$ and α^* .)

Note that $\dot{\equiv}_b \subseteq \dot{\equiv}_w$; we shall often implicitly use this property below.

A process expression is *indecomposable* if it is not behaviourally equivalent to $\mathbf{0}$ or a non-trivial parallel composition (a parallel composition is trivial if at least one of its components is behaviourally equivalent to $\mathbf{0}$). We say that a process theory has *unique parallel decomposition* if every process expression is behaviourally equivalent to a unique (generalised) parallel composition of indecomposable process expressions. Uniqueness means that the indecomposables of any two decompositions of a process expression are pairwise behaviourally equivalent up to a permutation.

We should make the definitions of indecomposable and unique parallel decomposition more formal and concrete for the two behavioural equivalences considered in this paper (viz. branching and weak bisimilarity). For reasons of generality and succinctness, however, it is convenient to postpone our formalisation until the next section, where we will discuss decomposition in the more abstract setting of commutative monoids. For now, we rely on the intuition of the reader and discuss informally and by means of examples to what extent the process theory introduced above might have the property of unique parallel decomposition. In our explanations we use branching bisimilarity as behavioural equivalence, but everything we say in the remainder of this section remains valid if branching bisimilarity is replaced by weak bisimilarity.

The first observation, already put forward by Milner and Moller in [15], is that there are process expressions which do not have a decomposition at all. (In [15], the following example is actually used to show that there exist infinite processes which do not have a decomposition modulo *strong* bisimilarity.)

Example 3. Consider the process expression $a^*\mathbf{0}$ (with $a \neq \tau$), and suppose that $a^*\mathbf{0}$ has a decomposition. Then, since $a^*\mathbf{0} \dot{\sim}_b P \parallel Q$ implies that either $P \dot{\sim}_b a^*\mathbf{0}$ or $Q \dot{\sim}_b a^*\mathbf{0}$, a decomposition of $a^*\mathbf{0}$ would necessarily include an indecomposable branching bisimilar to $a^*\mathbf{0}$. But, since $a^*\mathbf{0} \dot{\sim}_b a^*\mathbf{0} \parallel a^*\mathbf{0}$, there does not exist an indecomposable branching bisimilar to $a^*\mathbf{0}$. We conclude that $a^*\mathbf{0}$ fails to have a decomposition.

Note that the process expression $\alpha^*\mathbf{0}$ does not admit terminating behaviour; it does not have a transition sequence to a process expression from which no further transitions are possible. We want to identify a conveniently large subset of process expressions that do have decompositions, and to exclude the counterexample against existence of decompositions, we confine our attention to process expressions with terminating behaviour. Let us write $P \longrightarrow P'$ if there exists α such that $P \xrightarrow{\alpha} P'$; let us write $P \nrightarrow$ if there does not exist P' such that $P \longrightarrow P'$, and let us denote by \longrightarrow^* the reflexive-transitive closure of \longrightarrow .

Definition 4. A process expression P is *weakly normed* if there exists P' such that $P \longrightarrow^* P'$ and $P' \nrightarrow$.

For a weakly normed process expression we can define its weak norm as the length shortest complete transition sequence not counting τ transitions: For $a \in \mathcal{A}$ and weakly normed process expressions P and P' we write $P \xrightarrow{a} P'$ whenever there exist process expressions P' and Q' such that $P \longrightarrow P' \xrightarrow{a} Q' \longrightarrow P'$, and then we define the weak norm $wn(P)$ of P by

$$wn(P) = \min\{k : \exists P_0, \dots, P_k \in \mathcal{P}. \exists a_1, \dots, a_k \in \mathcal{A}. P = P_0 \xrightarrow{a_1} \dots \xrightarrow{a_k} P_k \nrightarrow\}.$$

It is immediate from their definitions that both branching and weak bisimilarity preserve weak norm: if two process expressions are branching or weakly bisimilar, then they have equal weak norms. It is also easy to establish that a parallel composition is weakly normed if, and only if, both parallel components are weakly normed. In fact, weak norm is additive with respect to parallel composition: the weak norm of a parallel composition is the sum of the weak norms of its parallel components.

Note that a process expression with weak norm 0 need not be behaviourally equivalent to $\mathbf{0}$, and such process expressions may still fail to have a decomposition. For instance, the argument in Example 3 that $a^*\mathbf{0}$ does not have a decomposition works just the same for $a^*\tau$, and the latter process expression has weak norm 0. By excluding the process expressions with weak norm 0 that are not behaviourally equivalent to $\mathbf{0}$, and also all the process expressions from which they can be reached, we secure the existence of decompositions.

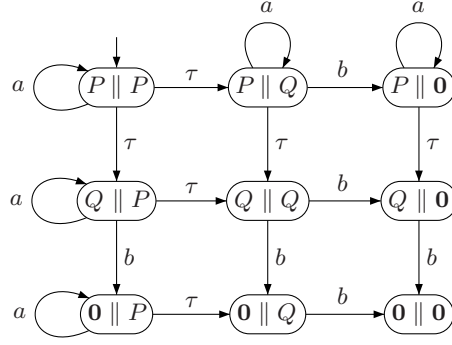


Figure 1: Transition graph associated with $P \parallel P$.

Definition 5. A weakly normed process expression P is *totally normed* if $P \rightarrow^* P'$ and $wn(P') = 0$ implies that P' is behaviourally equivalent to $\mathbf{0}$, for all weakly normed process expressions P' .

With a straightforward induction on weak norm it can be established that totally normed process expressions have a decomposition. But sometimes even more than one, as is illustrated in the following example.

Example 6. Consider the process expressions $P = a^*\tau.b.\mathbf{0}$ and $Q = b.\mathbf{0}$. It is clear that P and Q are *not* branching bisimilar. Both P and Q have weak norm 1, and from this it easily follows that they are both indecomposable. Note that, according to the operational semantics, $P \parallel P$ gives rise to the following three transitions:

1. $P \parallel P \xrightarrow{a} P \parallel P$;
2. $P \parallel P \xrightarrow{\tau} P \parallel Q$; and
3. $P \parallel P \xrightarrow{\tau} Q \parallel P$.

Further note that $P \parallel Q \xrightarrow{a} P \parallel Q$ and $Q \parallel P \xrightarrow{a} Q \parallel P$. (The complete transition graph associated with $P \parallel P$ by the operational semantics is shown in Figure 1.) Using these facts it is straightforward to verify that the symmetric closure of the binary relation

$$\mathcal{R} = \{(P \parallel P, P \parallel Q), (P \parallel P, Q \parallel P)\} \\ \cup \{(P \parallel Q, Q \parallel P), (P \parallel \mathbf{0}, \mathbf{0} \parallel P), (Q \parallel \mathbf{0}, \mathbf{0} \parallel Q)\}$$

is a branching bisimulation, and hence $P \parallel P \stackrel{b}{\sim} P \parallel Q$. It follows that $P \parallel P$ and $P \parallel Q$ are distinct decompositions of the same process up to branching bisimilarity.

Incidentally, the processes in the above counterexample also refute claims in [7] to the effect that processes definable with a totally normed BPP specification have a unique decomposition modulo branching bisimilarity and weak bisimilarity.

Apparently, more severe restrictions are needed.

Definition 7. Let $k \in \mathbb{N}$; a process expression P is *weakly bounded* by k if for all $\ell \in \mathbb{N}$ the existence of $P_1, \dots, P_\ell \in \mathcal{P}$ and $a_1, \dots, a_\ell \in \mathcal{A}$ such that $P \xrightarrow{a_1} \dots \xrightarrow{a_\ell} P_\ell$ implies that $\ell \leq k$. We say that P is *weakly bounded* if P is bounded by k for some $k \in \mathbb{N}$.

The *weak depth* $wd(P)$ of a weakly bounded process expression P is the length of its longest transition sequence not counting τ -transitions, i.e.,

$$wd(P) = \max\{k : \exists P_0, \dots, P_k. \exists a_1, \dots, a_k. P = P_0 \xrightarrow{a_1} \dots \xrightarrow{a_k} P_k\} .$$

Lemma 8. *Let P and Q be process expressions such that $P \xrightarrow{w} Q$. Then P is weakly bounded if, and only if, Q is weakly bounded, and, moreover, if P and Q are weakly bounded, then $wd(P) = wd(Q)$.*

In the remainder of this paper we shall establish that weakly bounded process expressions have a unique parallel decomposition both modulo branching and weak bisimilarity. We shall derive these results from a more general result about unique decomposition in commutative monoids.

3 Partial commutative monoids and decomposition

In this section we recall the abstract algebraic notion of partial commutative monoid, and formulate the property of unique decomposition. We shall see that the process theories discussed in the previous section give rise to commutative monoids of processes with parallel composition as binary operation. The notion of unique decomposition associated with these commutative monoids coincides with the notion of unique parallel decomposition as discussed.

Then, we shall recall the notion of decomposition order on partial commutative monoids proposed in [12]. We shall investigate whether the notion of decomposition order can be employed to prove unique parallel decomposition of weakly bounded process expressions modulo branching and weak bisimilarity.

Definition 9. A *commutative monoid* is a set M with a distinguished element e and a binary operation on M (for clarity in this definition denoted by \cdot) such that for all $x, y, z \in M$:

$$\begin{aligned} x \cdot (y \cdot z) &\simeq (x \cdot y) \cdot z && \text{(associativity);} \\ x \cdot y &\simeq y \cdot x && \text{(commutativity);} \\ x \cdot e &\simeq e \cdot x \simeq x && \text{(identity).} \end{aligned}$$

Henceforth, we adopt the convention that the symbol \cdot will be omitted if this is unlikely to cause confusion. Also, we shall sometimes use other symbols (\parallel , $+$, \dots) to denote the binary operation of a partial commutative monoid.

Remark 10. We adopt the convention that an expression designating an element of a partial commutative monoid M is defined only if all its subexpressions are defined. Thus, $x(yz)$ is defined only if yz is defined, say $yz = u$, and moreover xu is defined. Furthermore, if t_1 and t_2 are expressions and \mathcal{R} is a binary relation on M (e.g., equality or a partial order), then $t_1 \mathcal{R} t_2$ holds only if both t_1 and t_2 are defined and their values are related in \mathcal{R} . For instance, $x(yz) = (xy)z$ is true if the expressions $x(yz)$ and $(xy)z$ are both defined and their values are equal; otherwise it is false.

Note that the commutative law for a partial commutative monoid M could have been formulated thus: for all $x, y \in M$, xy is defined iff yx is defined, and if both xy and yx are defined then $xy = yx$. For a more succinct formulation we used in Definition 9 the symbol \simeq introduced by Kleene [11]: if t_1 and t_2 are expressions designating elements of M , then $t_1 \simeq t_2$ means that either t_1 and t_2 are both defined and have the same value, or t_1 and t_2 are both undefined.

We mention three key examples of partial commutative monoids that will serve to illustrate the theory of decomposition that we present in this paper.

- Example 11.** 1. It is well-known that the set of natural numbers \mathbf{N} is a commutative monoid¹ under addition. Each initial segment $\{0, \dots, n\}$ of \mathbf{N} is a partial commutative monoid with as partial binary operation the restriction of addition to $\{0, \dots, n\}$. So addition in the partial commutative monoid $\{0, \dots, n\}$ is defined for $k, l \in \{0, \dots, n\}$ iff $k + l \leq n$.
2. The set of positive natural numbers $\mathbf{N}_{>0}$ is a commutative monoid under multiplication.
3. Let X be any set. A (*finite*) *multiset* over X is a mapping $m : X \rightarrow \mathbf{N}$ such that $m(x) > 0$ for at most finitely many $x \in X$; the number $m(x)$ is called the *multiplicity* of x in m . The set of all multisets over X is denoted by $\mathcal{M}(X)$. If m and n are multisets, then their sum $m \uplus n$ is obtained by coordinatewise addition of multiplicities, i.e., $(m \uplus n)(x) = m(x) + n(x)$ for all $x \in X$. The *empty multiset* \square is the multiset that satisfies $\square(x) = 0$ for all $x \in X$. With these definitions, $\mathcal{M}(X)$ is a commutative monoid. If x_1, \dots, x_k is a sequence of elements of X , then $[x_1, \dots, x_k]$ denotes the multiset m such that $m(x)$ is the number of occurrences of x in x_1, \dots, x_k .

Process expressions modulo branching or weak bisimilarity also give rise to commutative monoids. Recall that $\underline{\simeq}_b$ and $\underline{\simeq}_w$ are equivalence relations on the set of process expressions. We denote the equivalence class of a process expression P modulo $\underline{\simeq}_b$ or $\underline{\simeq}_w$, respectively, by $[P]_b$ and $[P]_w$, i.e.,

$$[P]_b = \{Q \in \mathcal{P} : P \underline{\simeq}_b Q\} \text{ ; and}$$

$$[P]_w = \{Q \in \mathcal{P} : P \underline{\simeq}_w Q\} \text{ .}$$

Then, we define

$$\mathbf{B} = \mathcal{P} / \underline{\simeq}_b = \{[P]_b : P \in \mathcal{P}\} \text{ ; and}$$

$$\mathbf{W} = \mathcal{P} / \underline{\simeq}_w = \{[P]_w : P \in \mathcal{P}\} \text{ .}$$

In this paper, the similarities between the commutative monoids \mathbf{B} and \mathbf{W} will be more important than the differences. It will often be necessary to define very similar notions on both commutative monoids, in a very similar way. For succinctness of presentation, we allow ourselves a slight *abus de language* and most of the time deliberately omit the subscripts b and w from our notation for equivalence classes. Thus, we will be able to efficiently define notions and proof facts simultaneously for \mathbf{B} and \mathbf{W} .

For example, since both $\underline{\simeq}_b$ and $\underline{\simeq}_w$ are compatible with \parallel (see Equations (1) and (2)), we can define a binary operation \parallel simultaneously on \mathbf{B} and \mathbf{W} simply by

$$[P] \parallel [Q] = [P \parallel Q] \text{ ,}$$

by which we then mean to define a binary operation \parallel on \mathbf{B} and a binary relation \parallel on \mathbf{W} defined, respectively, by

$$[P]_b \parallel [Q]_b = [P \parallel Q]_b \text{ ; and}$$

$$[P]_w \parallel [Q]_w = [P \parallel Q]_w \text{ .}$$

Henceforth, we leave it to the reader to specialise notions, and also statements about them and their proofs, to \mathbf{B} and \mathbf{W} (or one of its submonoids to be introduced below).

We agree to write just $\mathbf{0}$ for $[\mathbf{0}]$. It is straightforward to establish that the binary operation \parallel is commutative and associative (both on \mathbf{B} and \mathbf{W}), and that $\mathbf{0}$ is the identity element for \parallel .

¹When the binary operation is everywhere defined, the adjective ‘partial’ is of course dropped.

Proposition 12. *The sets \mathbf{B} and \mathbf{W} are commutative monoids under \parallel , with $\mathbf{0}$ as identity element.*

Note that, by Lemma 8, whenever an equivalence class $[P]$ contains a weakly bounded process expression, it consists entirely of weakly bounded process expressions. We define subsets $\mathbf{B}_{fin} \subseteq \mathbf{B}_{tn} \subseteq \mathbf{B}$ and $\mathbf{W}_{fin} \subseteq \mathbf{W}_{tn} \subseteq \mathbf{W}$ by

$$\begin{aligned}\mathbf{B}_{fin} &= \mathcal{P} / \dot{\simeq}_b = \{[P]_b : P \in \mathcal{P} \text{ \& } P \text{ is weakly bounded}\} ; \\ \mathbf{B}_{tn} &= \mathcal{P} / \dot{\simeq}_b = \{[P]_b : P \in \mathcal{P} \text{ \& } P \text{ is totally normed}\} ; \\ \mathbf{W}_{fin} &= \mathcal{P} / \dot{\simeq}_w = \{[P]_w : P \in \mathcal{P} \text{ \& } P \text{ is weakly bounded}\} ; \text{ and} \\ \mathbf{W}_{tn} &= \mathcal{P} / \dot{\simeq}_w = \{[P]_w : P \in \mathcal{P} \text{ \& } P \text{ is totally normed}\} .\end{aligned}$$

It is straightforward to establish that a parallel composition is totally normed (weakly bounded) if, and only if, its parallel components are totally normed (weakly bounded).

Corollary 13. *The sets \mathbf{B}_{fin} and \mathbf{B}_{tn} are commutative submonoids of \mathbf{B} , and the sets \mathbf{W}_{fin} and \mathbf{W}_{tn} are commutative submonoids of \mathbf{W} .*

Notation 14. Let x_1, \dots, x_k be a (possibly empty) sequence of elements of a monoid M ; we define its *generalised product* $x_1 \cdots x_k$ inductively as follows:

- (i) if $n = 0$, then $x_1 \cdots x_k \simeq e$, and
- (ii) if $n > 0$, then $x_1 \cdots x_k \simeq (x_1 \cdots x_{k-1})x_k$.

Occasionally, we shall write $\prod_{i=1}^k x_i$ instead of $x_1 \cdots x_k$. Furthermore, we write x^n for the k -fold composition of x , i.e.,

$$x^k \simeq \prod_{i=1}^k x_i \text{ with } x_i = x \text{ for all } 1 \leq i \leq k.$$

It is straightforward by induction to establish the following *generalised associative law*:

$$(x_1 \cdots x_k)(y_1 \cdots y_\ell) \simeq x_1 \cdots x_k y_1 \cdots y_\ell .$$

Also by induction, a *generalised commutative law* can be established, so

$$\text{if } i_1, \dots, i_\ell \text{ is any permutation of } 1, \dots, \ell, \text{ then } x_1 \cdots x_\ell \simeq x_{i_1} \cdots x_{i_\ell} .$$

An indecomposable element of a commutative monoid is an element that cannot be written as a product of two elements that are both not the identity element of the monoid.

Definition 15. An element p of a commutative monoid M is called *indecomposable* if $p \neq e$ and $p = xy$ implies $x = e$ or $y = e$.

Example 16. 1. The number 1 is the only indecomposable element in \mathbf{N} and all its non-trivial initial segments; the trivial initial segment $\{0\}$ has no indecomposable elements.

2. The prime numbers are the indecomposable elements of $\mathbf{N}_{>0}$.

3. The indecomposable elements of $\mathcal{M}(X)$ are the *singleton* multisets, i.e., the multisets m for which it holds that $\sum_{x \in X} m(x) = 1$.

4. The indecomposable elements of \mathbf{B}_{fin} , \mathbf{B}_{tn} , \mathbf{B} , \mathbf{W}_{fin} , \mathbf{W}_{tn} , and \mathbf{W} are the equivalence classes of process expressions that are not behaviourally equivalent to $\mathbf{0}$ or a non-trivial parallel composition.

We define a decomposition in a partial commutative monoid to be a finite multiset of indecomposable elements. Note that this gives the right notion of equivalence on decompositions, for two finite multisets $\{x_1, \dots, x_k\}$ and $\{y_1, \dots, y_\ell\}$ are the same (extensionally) iff the sequence y_1, \dots, y_ℓ can be obtained from the sequence x_1, \dots, x_k by a permutation of its elements.

Definition 17. Let M be a partial commutative monoid. A *decomposition* in M is a finite multiset $\{p_1, \dots, p_k\}$ of indecomposable elements of M such that $p_1 \cdots p_k$ is defined. The element $p_1 \cdots p_k$ in M will be called the *composition* associated with the decomposition $\{p_1, \dots, p_k\}$, and, conversely, we say that $\{p_1, \dots, p_k\}$ is a decomposition of the element $p_1 \cdots p_k$ of M . Decompositions $d = \{p_1, \dots, p_k\}$ and $d' = \{p'_1, \dots, p'_\ell\}$ are *equivalent* in M (notation: $d \equiv d'$) if they have the same compositions, i.e., if

$$p_1 \cdots p_k = p'_1 \cdots p'_\ell .$$

A decomposition d in M is *unique* if $d \equiv d'$ implies $d = d'$ for all decompositions d' in M . We say that an element x of M has a unique decomposition if it has a decomposition and this decomposition is unique; we shall then denote the unique decomposition of x by ∂x . If every element of M has a unique decomposition, then we say that M has *unique decomposition*.

Example 18. 1. Since 1 is the only indecomposable element of \mathbf{N} and of any of its non-trivial initial segments, a decomposition in these partial commutative monoids is a multiset over the singleton set $\{1\}$. There is exactly one way in which a natural number n can be written as a sum of 1s, so decompositions in \mathbf{N} and its initial segments are unique.

2. According to the fundamental theorem of arithmetic every positive natural number has a unique decomposition in $\mathbf{N}_{>0}$.
3. Every finite multiset m over X has a unique decomposition in $\mathcal{M}(X)$, which contains for every $x \in X$ precisely $m(x)$ copies of the singleton multiset $\{x\}$.

The general notion of unique decomposition for commutative monoids, when instantiated to one of the commutative monoids of processes considered in this paper, indeed coincides with the notion of unique parallel decomposition as discussed in the preceding section. We have already seen that the commutative monoids \mathbf{B}_{tn} , \mathbf{B} , \mathbf{W}_{tn} and \mathbf{W} do not have unique decomposition. Our goal in the remainder of this paper is to establish that the commutative monoids \mathbf{B}_{fin} and \mathbf{W}_{fin} do have unique decomposition.

Preferably, we would like to have a general sufficient condition on partial commutative monoids for unique decomposition that is easily seen to hold for \mathbf{B}_{fin} and \mathbf{W}_{fin} , and hopefully also to other commutative monoids of processes. We shall now first recall the sufficient criterion put forward in [12], which was specifically designed for commutative monoids of processes. Then, we shall explain that it cannot directly be applied to conclude that \mathbf{B}_{fin} and \mathbf{W}_{fin} have unique decomposition. In the next section, we shall subsequently modify the condition, so that it becomes applicable to the commutative monoids at hand.

Definition 19. Let M be a partial commutative monoid; a partial order \preceq on M is a *decomposition order* if

- (i) it is *well-founded*, i.e., every nonempty subset of M has a \preceq -minimal element;
- (ii) the identity element e of M is the *least element* of M with respect to \preceq , i.e., $e \preceq x$ for all x in M ;
- (iii) it is *strictly compatible*, i.e., for all $x, y, z \in M$
if $x \prec y$ and yz is defined, then $xz \prec yz$;
- (iv) it is *precompositional*, i.e., for all $x, y, z \in M$
 $x \preceq yz$ implies $x = y'z'$ for some $y' \preceq y$ and $z' \preceq z$; and
- (v) it is *Archimedean*, i.e., for all $x, y \in M$
 $x^n \preceq y$ for all $n \in \mathbf{N}$ implies that $x = e$.

Remark 20. In [12] a slightly weaker form of the Archimedean property (condition (v) of Definition 19) was used. In the context of strict compatibility the weaker form was enough to arrive at a sufficient condition for unique decomposition in partial commutative monoids. We include the stronger version here, because we will need to relax the requirement of strict compatibility to just compatibility to facilitate application of our result in the present setting of weak behavioural equivalences.

In [12] it was proved that the existence of a decomposition order on a partial commutative monoid is a necessary and sufficient condition for unique decomposition. The advantage establishing unique decomposition via a decomposition order is that it circumvents first establishing cancellation, which in some cases is hard without knowing that the partial commutative monoid has unique decomposition. We refer to [12] for a more in-depth discussion.

In commutative monoids of processes, an obvious candidate decomposition order is the order induced on the commutative monoid by the transition relation. We define a binary relation \longrightarrow on \mathbf{B} and \mathbf{W} by

$$[P] \longrightarrow [P'] \text{ if there exist } Q \in [P], Q' \in [P'] \text{ and } \alpha \in \mathcal{A}_\tau \text{ such that } Q \xrightarrow{\alpha} Q'.$$

We shall denote the inverse of the reflexive-transitive closure of $(\longrightarrow^*)^{-1}$ (both on \mathbf{B} and \mathbf{W}) by \preceq .

Lemma 21. *If P and Q are process expressions such that $[Q] \preceq [P]$, then there exists $Q' \in [Q]$ such that $P \longrightarrow^* Q'$.*

The following lemma implies that every set of process expressions has minimal elements with respect to the reflexive-transitive closure of the transition relation. Note well that it holds true of our process calculus only thanks to the very limited facility of defining infinite behaviour, by means of simple loops.

Lemma 22. *If P_0, \dots, P_i, \dots ($i \in \mathbf{N}$) is an infinite sequence of process expressions, and $0, \dots, i, \dots$ ($i \in \mathbf{N}$) is an infinite sequence of elements in \mathcal{A}_τ such that $P_i \xrightarrow{i} P_{i+1}$ for all $i \in \mathbf{N}$, then there exists $j \in \mathbf{N}$ such that $P_k = P_\ell$ for all $k, \ell \geq j$.*

Proposition 23. *The relation \preceq is a well-founded precompositional partial order on each of the commutative monoids \mathbf{B} , \mathbf{B}_{tn} , \mathbf{B}_{fn} , \mathbf{W} , \mathbf{W}_{tn} , and \mathbf{W}_{fn} .*

Proof. That \preceq is reflexive and transitive is immediate from the definition.

That \preceq is well-founded, is, by Lemma 21, a straightforward consequence of Lemma 22.

It is well-known that a well-founded reflexive and transitive relation is a partial order, so it remains to establish that \preceq is precompositional. To this end, consider process expressions P , Q and R such that

$$[R] \preceq [P] \parallel [Q] .$$

Then, by Lemma 21, there exists $R' \in [R]$ such that $P \parallel Q \longrightarrow^* R'$. It is straightforward to establish by induction on the length of a transition sequence from $P \parallel Q$ to R' that there exist P' and Q' such that $R' = P' \parallel Q'$, $P \longrightarrow^* P'$ and $Q \longrightarrow^* Q'$. \square

Note that if the iteration prefix in our process calculus is replaced by any of the familiar more general forms of iteration or recursion, then \preceq as defined above will not be anti-symmetric, nor well-founded. Nevertheless, it is sometimes possible to define an anti-symmetric and well-founded partial order on processes based on the transition relation in a setting with a more general form of infinite behaviour, at least for totally normed processes. (See, e.g., [12] for an example of an anti-symmetric and well-founded order on normed processes definable in ACP with recursion, which is based on the restriction of the transition relation.)

The ordering \preceq defined on \mathbf{B}_{tn} , \mathbf{B} , \mathbf{W}_{tn} and \mathbf{W} is not a decomposition order: on \mathbf{B} and \mathbf{W}_{tn} it does not satisfy conditions (ii), (iii) and (v) of Definition 19, and on \mathbf{B}_{tn} and \mathbf{W}_{tn} it does not satisfy condition (iii) of Definition 19.

- Example 24.** 1. Since $a^*\mathbf{0} \xrightarrow{a} a^*\mathbf{0}$ is the only transition from $a^*\mathbf{0}$, it follows that $[a^*\mathbf{0}]$ is a minimal element. It is also clear that $[a^*\mathbf{0}] \neq \mathbf{0}$, so we have that $\mathbf{0}$ is not the least element of \preceq in \mathbf{B} and \mathbf{W} .
2. In Example 3 we have argued that $a^*\mathbf{0} = a^*\mathbf{0} \parallel a^*\mathbf{0}$, from which it easily follows that $[a^*\mathbf{0}]^n = [a^*\mathbf{0}]$ for all $n \in \mathbf{N}$. Hence, \preceq on \mathbf{B} and \mathbf{W} is not Archimedean.
3. Consider the process expressions $P = a^*\tau.b.\mathbf{0}$ and $Q = b.\mathbf{0}$ discussed in Example 6 (see also Figure 1). Then, since $P \xrightarrow{\tau} Q$ and $[P] \neq [Q]$, we have that $[Q] \prec [P]$, but also $[Q] \parallel [P] = [P] \parallel [P]$. It follows that \preceq is not strictly compatible.

In Examples 24.1 and 24.2, it is essential that $a^*\mathbf{0}$ is not totally normed. It can be established that in the commutative submonoids of totally normed process expressions modulo branching bisimilarity and weak bisimilarity the element $\mathbf{0}$ is the least element with respect to \preceq , and \preceq is Archimedean.

Proposition 25. *The partial order \preceq on \mathbf{B}_{tn} , \mathbf{B}_{fin} , \mathbf{W}_{tn} and \mathbf{W}_{fin} is Archimedean and $\mathbf{0}$ is its least element.*

We should now still ask ourselves the question whether \preceq on \mathbf{B}_{fin} and \mathbf{W}_{fin} is strictly compatible. Note that the important step towards proving the property for, e.g., \mathbf{B}_{fin} would be to establish, for all weakly bounded process expressions P , Q and R , the following implication:

$$P \xrightarrow{\tau} Q \ \& \ P \parallel R \dot{\preceq}_b Q \parallel R \implies P \dot{\preceq}_b Q .$$

Note that Example 24.3 illustrates that this implication does not hold for all totally normed processes, suggesting that the implication is perhaps hard to establish from first principles. In fact, all our attempts in this direction so far have failed. Note, however, that establishing the implication would be straightforward if we could use that \parallel is cancellative (i.e., $P \parallel R \dot{\preceq}_b Q \parallel R$ implies $P \dot{\preceq}_b Q$), and this, in turn, would be easy if we could use that \mathbf{B}_{fin} has unique decomposition.

The difficulty of establishing strict compatibility is really with strictness; it is straightforward to establish the following non-strict variant. Let M be a partial commutative monoid; a partial order \preceq on M is *compatible* if for all $x, y, z \in M$:

if $x \preceq y$ and yz is defined, then $xz \preceq yz$.

Proposition 26. *The partial order \preceq on \mathbf{B}_{tn} , \mathbf{B}_{fin} , \mathbf{W}_{tn} , and \mathbf{W}_{fin} is compatible.*

A partial order on a partial commutative monoid that has all the properties of a decomposition order except that it is compatible but not strictly compatible, we shall henceforth call a *weak decomposition order*.

Definition 27. Let M be a partial commutative monoid; a partial order \preceq on M is a *weak decomposition order* if it is well-founded, has the identity element $e \in M$ as least element, is compatible, precompositional and Archimedean.

The following proposition is an immediate corollary to Propositions 23, 25 and 26.

Proposition 28. *The partial order \preceq on \mathbf{B}_{tn} , \mathbf{B}_{fin} , \mathbf{W}_{tn} , and \mathbf{W}_{fin} is a weak decomposition order.*

In [12] it is proved that the existence of a decomposition order is a sufficient condition for a partial commutative monoid to have unique decomposition. Note that since \preceq is a weak decomposition order on \mathbf{B}_{tn} and \mathbf{W}_{tn} , and according to Example 6 these commutative monoids do not have unique decomposition, the existence of a *weak decomposition order* is *not* a sufficient condition for having unique decomposition; it should be supplemented with additional requirements to get a sufficient condition.

Strictness of compatibility—which is the only difference between the notion of decomposition order of [12] and the notion of weak decomposition order put forward here—is used both in the proof of *existence* of decompositions and in the proof that decompositions are *unique*. We shall now first establish the existence of decompositions in \mathbf{B} and \mathbf{W} separately. In the next section, we shall discuss uniqueness of decompositions in \mathbf{B} and \mathbf{W} . We shall propose a general subsidiary property that will allow us to establish uniqueness of decompositions in commutative monoids with a weak decomposition order, and establish that it holds in \mathbf{B} and \mathbf{W} .

Proposition 29. *In the commutative monoids \mathbf{B}_{tn} , \mathbf{B}_{fin} , \mathbf{W}_{tn} , and \mathbf{W}_{fin} every element has a decomposition.*

Proof. For \mathbf{B}_{tn} and \mathbf{W}_{tn} the proof is by induction on the weak norm; for \mathbf{B}_{fin} and \mathbf{W}_{fin} the proof is by induction on the weak depth. Below, we only give the proof for \mathbf{B}_{tn} and \mathbf{W}_{tn} .

Let P be a totally normed process expression; we prove with induction on the weak norm $wn(P)$ of P that $[P]$ has a decomposition.

If $wn(P) = 0$, then $[P] = \mathbf{0}$, which has the empty multiset of indecomposables as decomposition.

Suppose that $wn(P) > 0$, and suppose, by way of induction hypothesis, that all process expressions with a weak norm less than $wn(P)$ have a decomposition. We distinguish two cases. If $[P]$ is indecomposable, then the singleton multiset $\{[P]\}$ is a decomposition of $[P]$. If $[P]$ is not indecomposable, then there exist process expressions Q and R , not behaviourally equivalent to $\mathbf{0}$, such that P is behaviourally equivalent to $Q \parallel R$. Then, since Q and R are not behaviourally equivalent to $\mathbf{0}$, we have that $wn(Q), wn(R) > 0$. Hence, $[Q]$ and $[R]$ have decompositions, and the union of these decompositions is a decomposition of $[P]$. \square \square

4 Uniqueness

The failure of \preceq on \mathbf{B}_{fin} and \mathbf{W}_{fin} to be strictly compatible prevents us from getting our unique decomposition result for those commutative monoids as an immediate consequence of the result in [12]. Nevertheless, most of the ideas in the proof of uniqueness of decompositions in [12] can be adapted and reused in the context of a commutative monoids endowed with a weak decomposition order, albeit with the technical details slightly more involved. There is one special case in the unique decomposition proof that cannot be settled for commutative monoids with a weak decomposition order in general; this special case can be settled with an additional requirement on \preceq that is satisfied both in \mathbf{B}_{fin} and in \mathbf{W}_{fin} .

For the remainder of this paper, let M be a partial commutative monoid in which every element has a decomposition, and let \preceq be a weak decomposition order on M .

The decomposition extension of \preceq The uniqueness proof in [12] considers a minimal counterexample against unique decomposition, i.e., an element of the commutative monoid with at least two distinct decompositions, say d_1 and d_2 , that is \preceq -minimal in the set of all such elements. Then, an important technique in the proof is to select a particular indecomposable in one of the two decompositions and replace it by predecessors with respect to the decomposition order. From minimality together with strict compatibility it is then concluded that the resulting decomposition is unique, which plays a crucial role in subsequent arguments towards a contradiction. To avoid the use of strict compatibility, we need a more sophisticated notion of minimality for the considered counterexample. The idea is to not just pick a \preceq -minimal element among the elements with two or more decompositions; we also choose the presupposed pair of distinct decompositions (d_1, d_2) in such a way that it is minimal with respect to a well-founded ordering induced by \preceq on pairs of decompositions.

First, we define some further notation on multisets: Let X be a set. If m and n are multisets over x , then we write $m - n$ for the multiset difference of m and n , i.e., for all $x \in X$,

$$m - n = \begin{cases} m(x) - n(x) & \text{if } m(x) \geq n(x) ; \\ 0 & \text{otherwise .} \end{cases}$$

Then, we define the *decomposition extension* \triangleleft of \prec by $d \triangleleft d'$ if, and only if, there exist, for some $k \geq 1$, a sequence of indecomposables $p_1, \dots, p_k \in M$, a sequence $x_1, \dots, x_k \in M$, and a sequence of decompositions d_1, \dots, d_k such that

- (i) $x_i \prec p_i$ ($1 \leq i \leq k$);
- (ii) each d_i is a decomposition of x_i ($1 \leq i \leq k$); and
- (iii) $d = (d' - \downarrow p_1, \dots, p_k) \uplus (d_1 \uplus \dots \uplus d_k)$.

We write $d \trianglelefteq d'$ if $d = d'$ or $d \triangleleft d'$. Note that if $d \trianglelefteq d'$, x is the composition of d , and y is the composition of d' , then, by compatibility, $x \preceq y$.

Lemma 30. *The partial order \trianglelefteq on decompositions is well-founded.*

Proof. It suffices to note that \trianglelefteq is included in the standard multiset ordering associated with the well-founded partial order \preceq , which is proved to be well-founded by Dershowitz and Manna in [5]. \square \square

In our uniqueness proof, we shall use the well-foundedness of both \preceq and the Cartesian order \trianglelefteq_{\times} induced on pairs of decompositions by \trianglelefteq . For two pairs of

decompositions (d_1, d_2) and (d'_1, d'_2) , we write $(d_1, d_2) \trianglelefteq_\times (d'_1, d'_2)$ if $d_1 \trianglelefteq d'_1$ and $d_2 \trianglelefteq d'_2$. A pair of decompositions (d_1, d_2) is said to be a *counterexample* against unique decomposition if d_1 and d_2 are distinct but equivalent, i.e., if $d_1 \equiv d_2$, but not $d_1 = d_2$. A counterexample (d_1, d_2) against unique decomposition is *minimal* if it is both minimal with respect to \preceq and minimal with respect to \trianglelefteq_\times . That is, a counterexample (d_1, d_2) against unique decomposition is *minimal* if

1. all \preceq -predecessors of the (common) composition of d_1 and d_2 have a unique decomposition; and
2. for all (d'_1, d'_2) such that $(d'_1, d'_2) \trianglelefteq_\times (d_1, d_2)$ and $(d'_1, d'_2) \neq (d_1, d_2)$ it holds that $d'_1 \equiv d'_2$ implies $d'_1 = d'_2$.

If unique decomposition would fail then there would exist a minimal counterexample. For, the subset of processes with two or more decompositions is nonempty, and therefore, by well-foundedness of \preceq , it has a \preceq -minimal element, say x . Then, by well-foundedness of \trianglelefteq_\times on pairs of decompositions, the nonempty set of pairs of distinct decompositions with x as their composition has a minimal element, say (d_1, d_2) . Note that (d_1, d_2) is \trianglelefteq_\times -minimal in the set of *all* counterexamples against unique decomposition, it suffices to note that if $(d'_1, d'_2) \trianglelefteq_\times (d_1, d_2)$ and $(d'_1, d'_2) \neq (d_1, d_2)$, then the (common) composition y associated with d'_1 and d'_2 satisfies $y \preceq x$ by compatibility.

The general idea of the proof is that we derive a contradiction from the assumption that there exists a minimal counterexample (d_1, d_2) against unique decomposition. The decompositions d_1 and d_2 should be distinct, so the set of indecomposables that occur more often in one of the decompositions than in the other is nonempty. This set is clearly also finite, so it has \preceq -maximal elements. We declare p to be such an \preceq -maximal element, and assume, without loss of generality, that p occurs more often in d_1 than in d_2 . Then we have that

- (A) $d_1(p) > d_2(p)$; and
- (B) $d_1(q) = d_2(q)$ for all indecomposables q such that $p \prec q$.

We shall distinguish two cases, based on how the difference between d_1 and d_2 manifests itself, and derive a contradiction in both cases:

1. $d_1(p) > d_2(p) + 1$ or $d_1(q) \neq 0$ for some indecomposable q distinct from p ; we refer to this case by saying that d_1 and d_2 are *too far apart*.
2. $d_1(p) = d_2(p) + 1$ and $d_1(q) = 0$ for all q distinct from p ; we refer to this case by saying that d_1 and d_2 are *too close together*.

Case 1: d_1 and d_2 are too far apart In this case, either the multiplicity of p in d_1 exceeds the multiplicity of p in d_2 by at least 2, or the difference in multiplicities is 1 but there is another indecomposable q , distinct from p , in d_1 . We argue that d_1 has a predecessor d' in which p occurs more often than in any predecessor of d_2 , while, on the other hand, the choice of a minimal counterexample implies that every predecessor of d_1 is also a predecessor of d_2 . (The arguments leading to a contradiction in this case are analogous to the arguments in the proof in [12]; the only difference is the use of the ordering \trianglelefteq instead of \preceq .)

Using that \preceq is compatible and Archimedean, it can be established that there is a bound on the multiplicity of p in the predecessors of d_1 .

Lemma 31. *The set $\{d'_1(p) : d'_1 \triangleleft d_1\}$ is finite.*

Proof. Denote by y the composition of d_1 . Clearly, if d'_1 is a predecessor of d_1 , then, by compatibility, we have that $p^n \preceq y$ for all $n \leq d'_1(p)$. Hence, if the set $\{d'_1(p) : d'_1 \triangleleft d_1\}$ would *not* be finite, then $p^n \preceq y$ for all $n \in \mathbf{N}$, from which, since \preceq is Archimedean, it would follow that $p = e$. But $p = e$ is in contradiction with the assumption that p is indecomposable. \square \square

Let m be the maximum of the multiplicities of p in predecessors of d_1 , i.e.,

$$m := \max\{d'_1(p) : d'_1 \triangleleft d_1\} . \quad (3)$$

On the one hand, if $d_1(p) > d_2(p) + 1$, then $d_1 - \wr p \triangleleft d_1$, so $m \geq d_1(p) - 1 > d_2(p)$. On the other hand, if $d_1(q) \neq 0$ for some indecomposable $q \neq p$, then $d_1 - \wr q \triangleleft d_1$, so $m \geq d_1(p) > d_2(p)$. Hence

$$d_2(p) < m . \quad (4)$$

Lemma 32. *For every $d'_1 \trianglelefteq d_1$ there exists $d'_2 \trianglelefteq d_2$ such that $d'_1 \equiv d'_2$.*

Proof. Let $d'_1 \trianglelefteq d_1$. Clearly, if $d'_1 = d_1$, then we can take $d'_2 = d_2$ and immediately get $d'_1 = d_1 \equiv d_2 = d'_2$. So suppose that $d'_1 \triangleleft d_1$. Then there exist a decomposition d''_1 and, for some $k \geq 1$, sequences of indecomposables p_1, \dots, p_k and of decompositions $d_{1,1}, \dots, d_{1,k}$ such that

- (i) $d_1 = d''_1 \uplus \wr p_1, \dots, p_k$;
- (ii) each $d_{1,i}$ is a decomposition of a predecessor of p_i ($1 \leq i \leq k$); and
- (iii) $d'_1 = d''_1 \uplus d_{1,1} \uplus \dots \uplus d_{1,k}$.

Denote by x, x', x'' , and x_i ($1 \leq i \leq k$) the compositions of the decompositions d_1, d'_1, d''_1 and $d_{1,i}$ ($1 \leq i \leq k$), respectively. Then, for all $1 \leq i \leq k$, x_i is a \preceq -predecessor of p_i , so, by compatibility,

$$x' = x''x_1 \cdots x_k \preceq x''p_1 \cdots p_k = x .$$

If $x' = x$, then $d'_1 \equiv d_2$, so we can take $d'_2 = d_2$ and get $d'_1 \equiv d'_2$.

It remains to consider the case that $x' \prec x$. Let q_1, \dots, q_ℓ be such that $d_2 = \wr q_1, \dots, q_\ell$. Then, since x is the composition of d_1 and $d_1 \equiv d_2$, $x = q_1 \cdots q_\ell$, and hence, by precompositionality, there exist x'_1, \dots, x'_ℓ such that $x' = x'_1 \cdots x'_\ell$ and $x'_i \preceq q_i$ ($1 \leq i \leq \ell$). Note that, since $x' \neq x$, there is at least one $1 \leq i \leq \ell$ such that $x'_i \neq q_i$. We assume without loss of generality that the indecomposables q_1, \dots, q_ℓ and their weak predecessors x'_1, \dots, x'_ℓ are ordered in such a way that there exists $1 \leq j \leq \ell$ such that $x'_i = q_i$ for all $1 \leq i < j$, and $x'_i \prec q_i$ for all $j \leq i \leq \ell$. Let $d'_{2,j}, \dots, d'_{2,\ell}$ be decompositions of x'_j, \dots, x'_ℓ , and define $d'_2 = \wr q_1, \dots, q_{j-1} \uplus d'_{2,j} \uplus \dots \uplus d'_{2,\ell}$. Then $d'_2 \triangleleft d_2$, and since d'_1 and d'_2 both have x' as their composition, we have that $d'_1 \equiv d'_2$. \square \square

If $k \in \mathbf{N}$, then we write $k \cdot \wr p$ for the decomposition consisting of k occurrences of p , i.e., the multiset for which it holds that

$$(k \cdot \wr p)(q) = \begin{cases} k & \text{if } q = p ; \\ 0 & \text{otherwise} . \end{cases}$$

From (3) it is clear that $m \cdot \wr p \triangleleft d_1$. Hence, by Lemma 32, there exists $d'_2 \trianglelefteq d_2$ such that $m \cdot \wr p \equiv d'_2$. Since (d_1, d_2) is a minimal counterexample, it follows that $m \cdot \wr p = d'_2$, and hence $m \cdot \wr p \trianglelefteq d_2$. Moreover, from (4), it is clear that $m \cdot \wr p \neq d_2$, so $m \cdot \wr p \triangleleft d_2$. Thus, we now have

$$m \cdot \wr p \triangleleft d_1, d_2 . \quad (5)$$

We now proceed to argue that indecomposables distinct from p in d_2 can be used to create $m - d_2(p)$ additional occurrences of p in predecessors of d_2 . Since those extra occurrences of p can only be created by occurrences in d_2 of indecomposables q such that $p \prec q$, it can be concluded by assumption B that d_1 must have the same potential for creating extra occurrences of p . We shall see that this reasoning will eventually lead to a contradiction with our definition of m as the maximal number of occurrences of p in predecessors of d_1 .

In the remainder of our argument, it will be convenient to have notation for specific parts of d_1 and d_2 : For $i = 1, 2$ we denote by $d_i^{\succ p}$ the multiset consisting of all indecomposables q in d_i such that $p \prec q$, i.e., $d_i^{\succ p}$ is defined by

$$d_i^{\succ p}(q) = \begin{cases} d_i(q) & \text{if } q \succ p ; \\ 0 & \text{otherwise ;} \end{cases}$$

we denote by $d_i^{\overline{p}}$ the multiset consisting of all occurrences of p in d_i , i.e., $d_i^{\overline{p}}$ is defined by

$$d_i^{\overline{p}}(q) = \begin{cases} d_i(q) & \text{if } q = p ; \\ 0 & \text{otherwise ;} \end{cases}$$

we denote by $d_i^{\not\succ p}$ the multiset consisting of all occurrences of p in d_i , i.e., $d_i^{\not\succ p}$ is defined by

$$d_i^{\not\succ p}(q) = \begin{cases} d_i(q) & \text{if } q \not\succ p ; \\ 0 & \text{otherwise .} \end{cases}$$

Then clearly we have

$$d_i = d_i^{\succ p} \uplus d_i^{\overline{p}} \uplus d_i^{\not\succ p} \quad (i = 1, 2) .$$

That the decompositions $d_i^{\succ p}$ ($i = 1, 2$) both incorporate the potential of creating $m - d_2(p)$ occurrences of p is formalised by proving that $(m - d_2(p)) \cdot \downarrow p \downarrow \triangleleft d_i^{\succ p}$ ($i = 1, 2$). We shall first prove $(m - d_2(p)) \cdot \downarrow p \downarrow \triangleleft d_2^{\succ p}$, and for this we need the following general lemma.

Lemma 33. *Let M be a partial commutative monoid with a weak decomposition order \preceq in which every element has at least one decomposition. Let $x, y, z \in M$, and suppose that xy has a unique decomposition. Then*

$$xy \prec xz \text{ implies } y \prec z .$$

Proof. Suppose that $xy \prec xz$; we prove with induction on the cardinality of the unique decomposition ∂x of x that $y \preceq z$. Note that it then immediately follows that $y \prec z$, for $y = z$ would imply $xy = xz$.

If ∂x is the empty multiset, then $x = e$, and hence, $y = xy \prec xz = z$.

Suppose that ∂x is non-empty, let p be an indecomposable in ∂x , and let x' be the composition of $\partial x - \downarrow p \downarrow$. Then $x = px'$, so

$$px'y = xy \prec xz = px'z . \quad (6)$$

Hence, by precompositionality, there exist $u \preceq p$ and $v \preceq x'z$ such that $px'y = uv$. Since xy has a unique decomposition and $uv = xy$, also u and v have unique decompositions ∂u and ∂v , respectively. Moreover, since p is an element of $\partial(xy)$, either $p \in \partial u$ or $p \in \partial v$. On the one hand, if $p \in \partial u$, then $p \preceq u$, and since also $u \preceq p$, it follows that $u = p$, and hence $x'y = v \preceq x'z$. On the other hand, if $p \in \partial v$, then there exists v' such that $v = pv'$, and hence, by compatibility,

$x'y = uv' \preceq pv' = v \preceq x'z$. In both cases, we have derived $x'y \preceq x'z$, and since $x'y = x'z$ cannot be the case in view of (6), we have that

$$x'y \prec x'z \text{ .}$$

Note that $\partial x - \wr p$ is the unique decomposition of x' and that its cardinality is less than the cardinality of ∂x . So it now follows by the induction hypothesis $y \preceq z$. \square \square

Let $x = p^{d_2(p)}$ and $y = p^{m-d_2(p)}$, and denote by z the composition of $d_2^{\prec p} \uplus d_2^{\not\prec p}$. Then $xy = p^m$ and xz is equal to the composition of both d_1 and d_2 . Note that from (5) and the minimality of the counterexample (d_1, d_2) it immediately follows that $p^m = xy \prec xz$. (For if $xy = xz$, then $p^m = xz$, so both $(m \cdot \wr p, d_2)$ and $(d_1, m \cdot \wr p)$ would constitute smaller counterexamples.) It follows that xy has a unique decomposition, so by Lemma 33 it follows that $y \prec z$. By precompositionality, y has a decomposition, say d'_2 such that $d'_2 \prec d_2^{\prec p} \uplus d_2^{\not\prec p}$, and since y , in fact, has a unique decomposition, it follows that $(m - d_2(p)) \cdot \wr p \triangleleft d_2^{\prec p} \uplus d_2^{\not\prec p}$. By definition of $d_2^{\not\prec p}$, p does not occur in $d_2^{\not\prec p}$, nor in any decomposition of a predecessor of an indecomposable in $d_2^{\not\prec p}$, so $(m - d_2(p)) \cdot \wr p \triangleleft d_2^{\prec p}$. Since $d_2^{\prec p} = d_1^{\prec p}$ according to assumption B, we have $(m - d_2(p)) \cdot \wr p \triangleleft d_1^{\prec p}$. It follows that

$$(m - d_2(p) + d_1(p)) \cdot \wr p \triangleleft d_1 \text{ ,} \quad (7)$$

and since $d_2(p) < d_1(p)$ according to assumption A, we find $m - d_2(p) + d_1(p) > m$. We conclude that (7) contradicts our definition of m in (3) as the maximum of the multiplicities of p in the predecessors of d_1 .

Case 2: d_1 and d_2 are too close together In this case d_1 contains no other indecomposables than p , while d_2 has $d_1(p) - 1$ occurrences of p supplemented with a multiset d'_2 of other indecomposables

In [12] it is proved, via a sophisticated argument, that the composition of d'_2 is a \preceq -predecessor of p . Hence, by strict compatibility, the composition of d_2 is an \preceq -predecessor of d_1 , which is in contradiction with the assumption that the decompositions d_1 and d_2 are equivalent.

That \preceq is not strictly compatible, but just compatible, leaves the possibility that d_1 and d_2 are equivalent even if the composition of d'_2 is a predecessor of p . For \mathbf{B}_{fin} and \mathbf{W}_{fin} this possibility can be ruled out by noting that the composition of d'_2 can be reached from p by τ -transitions, and proving that every transition of p can be simulated by a transition of the composition of d'_2 . The following notion formalises this reason in the abstract setting of commutative monoids with a weak decomposition order.

Definition 34. Let M be a partial commutative monoid, and let \preceq be a weak decomposition order on M . We say that \preceq satisfies *power cancellation* if for all $x, y \in M$, for every indecomposable $p \in M$ such that $p \not\prec x, y$, and for all $k \in \mathbb{N}$ it holds that $p^k x = p^k y$, then $x = y$.

Suppose that \preceq on M has power cancellation, let $k = d_2(p)$ and let x be the composition of d'_2 . Then from $d_1 \equiv d_2$ it follows that

$$p^k p = p^k x \text{ .}$$

Clearly, $p \not\prec p$ and, since d'_2 consists of indecomposables q such that $p \not\prec q$, it follows that also $p \not\prec x$. Hence, since \preceq has power cancellation, $p = x$, so $d'_2 = \wr p$. It follows that $d_1 = d_2$, which contradicts that (d_1, d_2) is a counterexample against unique decomposition.

Theorem 35. *Let M be a commutative monoid with a weak decomposition order that satisfies power cancellation. If every element of M has a decomposition, then M has unique decomposition.*

In the previous section we have already established that in the commutative monoids \mathbf{B}_{fin} and \mathbf{W}_{fin} every element has a decomposition and that \preceq is a weak decomposition order on \mathbf{B}_{fin} and \mathbf{W}_{fin} . To be able to conclude from Theorem 35 that \mathbf{B}_{fin} and \mathbf{W}_{fin} have unique decomposition, it remains to establish that \preceq on these commutative monoids satisfies power cancellation.

Proposition 36. *The weak decomposition order \preceq on \mathbf{B}_{fin} and \mathbf{W}_{fin} satisfies power cancellation.*

Proof. We present the proof for \mathbf{B}_{fin} ; the proof for \mathbf{W}_{fin} is very similar except that some details are slightly simpler.

Let p be an indecomposable element in \mathbf{B}_{fin} , and let x , y and z be elements of \mathbf{B}_{fin} such that $p \not\prec x, y$, and, for some $k \in \mathbf{N}$,

$$z = p^k x = p^k y ; \quad (8)$$

we need to prove that $x = y$.

To this end, we first note that the ordering \preceq on $\mathbf{B}_{fin} \times \mathbf{B}_{fin} \times \mathbf{B}_{fin}$ defined by

$$(u', v', w') \preceq (u, v, w) \text{ if } u' \preceq u \text{ and whenever } u' = u \text{ then also } v' \preceq v \text{ and } w' \preceq w$$

is well-founded. We proceed by \preceq -induction on (z, x, y) , and suppose, by way of induction hypothesis, that whenever $(z', x', y') \preceq (z, x, y)$ and, for some indecomposable element p' of \mathbf{B}_{fin} , $z' = (p')^\ell x' = (p')^\ell y'$, then $x' = y'$.

Note that x and y are non-empty sets of process expressions, and that, to prove $x = y$, it suffices to show that there exist process expressions $Q \in x$ and $R \in y$ such that $Q \dot{\sim}_b R$. By Lemma 22, the non-empty sets of process expressions x and y have minimal elements with respect to the ordering induced on process expressions by $(\xrightarrow{\tau})^*$. Let Q and R be $(\xrightarrow{\tau})^*$ -minimal elements in x and y , respectively; we prove that $Q \dot{\sim}_b R$ by establishing that the binary relation

$$\mathcal{R} = \{(Q, R), (R, Q)\} \cup \dot{\sim}_b$$

is a branching bisimulation.

To this end, we first suppose that $Q \xrightarrow{\alpha} Q'$ for some Q' , and prove that there exist R'' and R' such that $R \twoheadrightarrow R'' \xrightarrow{(\alpha)} R'$, $Q \mathcal{R} R''$, and $Q' \mathcal{R} R'$.

Let P be an element of p , denote by P^k the k -fold parallel composition of P , and let $z' = [P^k \parallel Q']_b$. Then $z' \preceq z$, so we can distinguish two cases:

CASE 1: Suppose that $z' = z$. Then, since $P^k \parallel Q$ is weakly bounded, it follows that $\alpha = \tau$. Let $x' = [Q']_b$; since Q is a minimal element of x , we have that $x' \prec x$. Hence, $(z', x', y) \prec (z, x, y)$, so by the induction hypothesis $[Q']_b = x' = y = [R]_b$. It follows that $Q' \dot{\sim}_b R$, and we can take $R'' = R' = R$.

CASE 2: Suppose that $z' \prec z$. Then, by the induction hypothesis, \preceq on the partial commutative submonoid $\{z'' : z'' \preceq z'\}$ of \mathbf{B} satisfies power cancellation. By Theorem 35, it follows that z' has a unique decomposition. From $Q \xrightarrow{\alpha} Q'$ it follows that

$$P^k \parallel Q \xrightarrow{\alpha} P^k \parallel Q' ,$$

and hence, since $P^k \parallel Q \dot{\sim}_b P^k \parallel R$ according to (8), there exist R' , R'' , S' , and S'' such that

$$P^k \parallel R \twoheadrightarrow S'' \parallel R'' \xrightarrow{(\alpha)} S' \parallel R' ,$$

with $P^k \parallel Q \dot{\hookrightarrow}_b S'' \parallel R''$ and $P^k \parallel Q' \dot{\hookrightarrow}_b S' \parallel R'$. We have that

$$[R']_b \preceq [R'']_b \preceq [R]_b$$

and

$$[S']_b \preceq [S'']_b \preceq [P^k]_b,$$

and, since $[S']_b \parallel [R']_b = z' \neq z = [P^k \parallel R]_b$, it also holds that $[R']_b \neq [R]_b$, or $[S']_b \neq [P^k]_b$. We distinguish two subcases:

CASE 1.1: Suppose $[R']_b \prec [R]_b$. Then, since $p \not\prec x = [R]_b$, the unique decomposition of $[R']_b$ cannot have occurrences of p . Since z' has k occurrences of p , it follows that $p^k \preceq [S']_b \preceq [S'']_b \preceq [P^k]_b = p^k$, so $[S']_b = [S'']_b = [P^k]_b$. Since $z' = p^k \parallel [Q']_b = p^k \parallel [R']_b$, by the induction hypothesis $[Q']_b = [R']_b$, and hence $Q' \mathcal{R} R'$.

It remains to establish that $Q \mathcal{R} R''$. If $R'' = R$, then, since $Q \mathcal{R} R$, this is immediate. If $R'' \neq R$, then since R is a $(\xrightarrow{\tau})^*$ -minimal element of y , it follows that $[R'']_b \prec [R]_b$, so from $z = p^k \parallel [Q]_b = p^k \parallel [R'']_b$ it follows by the induction hypothesis that $[Q]_b = [R'']_b$, and hence $Q \mathcal{R} R''$.

CASE 1.2: Suppose $[S']_b \prec [P^k]_b$. Then the multiplicity of p in the unique decomposition of $[S']_b$ is at most $k - 1$. It follows that p must be an element of $[R']_b$. This means that $p \preceq [R']_b$, and since $p \not\prec y = [R]_b$, we can conclude that $P \dot{\hookrightarrow}_b R' \dot{\hookrightarrow}_b R'' \dot{\hookrightarrow}_b R$. Thus, we also get that the multiplicity of p in $[S']_b$ is, in fact, $k - 1$, and therefore we can assume without loss of generality that there exist process expressions $P_1, P_2, \dots, P_k, P_1'$ such that

$$\begin{aligned} S'' &= P_1 \parallel P_2 \parallel \dots \parallel P_k, \\ S' &= P_1' \parallel P_2 \parallel \dots \parallel P_k, \\ P &\longrightarrow P_i \quad (1 \leq i \leq k), \\ P &\dot{\hookrightarrow}_b P_i \quad (2 \leq i \leq k), \text{ and} \\ P_1 &\xrightarrow{(\alpha)} P_1'. \end{aligned}$$

From $P^k \parallel Q' \dot{\hookrightarrow}_b R \parallel P_2 \parallel \dots \parallel P_k \parallel P_1'$, $P \dot{\hookrightarrow}_b R$, and $P \dot{\hookrightarrow}_b P_i$ ($2 \leq i \leq k$) it follows that $Q' \dot{\hookrightarrow}_b P_1'$. Hence, since $P \dot{\hookrightarrow}_b R$, there exist R_1, R_1' such that $R \longrightarrow R_1 \xrightarrow{(\alpha)} R_1'$, $P_1 \dot{\hookrightarrow}_b R_1$, and $P_1' \dot{\hookrightarrow}_b R_1'$. From $Q' \dot{\hookrightarrow}_b P_1' \dot{\hookrightarrow}_b R_1'$ it follows that $Q' \mathcal{R} R_1'$.

It remains to establish that $Q \mathcal{R} R_1$. If $R_1 = R$, then, since $Q \mathcal{R} R$, this is immediate. If $R_1 \neq R$, then, since R is a $(\xrightarrow{\tau})^*$ -minimal element of y , it follows that $[P_1]_b = [R_1]_b \prec [R]_b = [P]_b$. So from $z = p^k \parallel [Q]_b = p^k \parallel [P_1]_b$ it follows by the induction hypothesis that $Q \dot{\hookrightarrow}_b P_1 \dot{\hookrightarrow}_b R_1$, and hence $Q \mathcal{R} R_1$.

In a completely analogous manner, it can be established that whenever $R \xrightarrow{\alpha} R'$ for some process expression R' , then there exist process expressions Q' and Q'' such that $Q \longrightarrow Q'' \xrightarrow{(\alpha)} Q'$, $R \mathcal{R} Q''$, and $R' \mathcal{R} Q'$.

We conclude that \mathcal{R} is a branching bisimulation, and hence $Q \dot{\hookrightarrow}_b R$. $\square \quad \square$

By Propositions 28, 29 and 36, the commutative monoids \mathbf{B}_{fin} and \mathbf{W}_{fin} are endowed with a weak decomposition order \preceq satisfying power cancellation, and, moreover, all elements of \mathbf{B}_{fin} and \mathbf{W}_{fin} have at least one decomposition. Hence, by Theorem 35, we get the following corollary.

Corollary 37. *The commutative monoids \mathbf{B}_{fin} and \mathbf{W}_{fin} have unique decomposition.*

5 Concluding remarks

We have presented a general sufficient condition on partial commutative monoids that implies the property of unique decomposition, and is applicable to commutative monoids of behaviour incorporating a notion of unobservability. We have chosen to illustrate the application of our condition in the context of a very simple process calculus with an operation for pure interleaving as parallel composition. We expect, however, that our condition can also be used to prove unique decomposition results in more complicated settings (e.g., (finite) fragments of π -calculus). We leave it for future work to verify this claim.

References

- [1] L. Aceto, W. J. Fokkink, A. Ingólfssdóttir, and B. Luttik. A finite equational base for CCS with left merge and communication merge. *ACM Trans. Comput. Log.*, 10(1), 2009.
- [2] T. Basten. Branching bisimilarity is an equivalence indeed! *Information Processing Letters*, 58(3):141–147, 1996.
- [3] S. Christensen. *Decidability and Decomposition in Process Algebras*. PhD thesis, University of Edinburgh, 1993.
- [4] F. Corradini, R. Gorrieri, and D. Marchignoli. Towards parallelization of concurrent systems. *RAIRO Inform. Théor. Appl.*, 32(4-6):99–125, 1998.
- [5] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Commun. ACM*, 22(8):465–476, 1979.
- [6] W. J. Fokkink and B. Luttik. An *omega*-complete equational specification of interleaving. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *ICALP*, volume 1853 of *Lecture Notes in Computer Science*, pages 729–743. Springer, 2000.
- [7] S. Fröschle and S. Lasota. Normed processes, unique decomposition, and complexity of bisimulation equivalences. *Electronic Notes in Theoretical Computer Science*, 239:17 – 42, 2009. Joint Proceedings of the 8th, 9th, and 10th International Workshops on Verification of Infinite-State Systems (INFINITY 2006, 2007, 2008).
- [8] R. J. van Glabbeek and W. P. Weijland. Branching time and abstraction in bisimulation semantics. *J. ACM*, 43(3):555–600, 1996.
- [9] J. F. Groote and F. Moller. Verification of parallel systems via decomposition. In R. Cleaveland, editor, *CONCUR*, volume 630 of *Lecture Notes in Computer Science*, pages 62–76. Springer, 1992.
- [10] Y. Hirshfeld and M. Jerrum. Bisimulation equivalence is decidable for normed process algebra. In Jirí Wiedermann, Peter van Emde Boas, and Mogens Nielsen, editors, *ICALP*, volume 1644 of *Lecture Notes in Computer Science*, pages 412–421. Springer, 1999.
- [11] S. C. Kleene. *Introduction to Metamathematics*. D. Van Nostrand Co., Inc., New York, N. Y., 1952.
- [12] B. Luttik and V. van Oostrom. Decomposition orders—another generalisation of the fundamental theorem of arithmetic. *Theor. Comput. Sci.*, 335(2-3):147–186, 2005.

- [13] R. Milner. *Communication and Concurrency*. Prentice-Hall International, 1989.
- [14] R. Milner. Operational and algebraic semantics of concurrent processes. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, pages 1201–1242. The MIT Press, 1990.
- [15] R. Milner and F. Moller. Unique decomposition of processes. *Theoret. Comput. Sci.*, 107:357–363, January 1993.
- [16] F. Moller. *Axioms for Concurrency*. PhD thesis, University of Edinburgh, 1989.
- [17] F. Moller. The importance of the left merge operator in process algebras. In Mike Paterson, editor, *ICALP*, volume 443 of *Lecture Notes in Computer Science*, pages 752–764. Springer, 1990.
- [18] F. Moller. The nonexistence of finite axiomatisations for CCS congruences. In *Proceedings of LICS'90*, pages 142–153. IEEE Computer Society Press, 1990.